END USER SERVICES PROGRAM OFFICE

End User Services Program Office

NASA-STD-2804 – Minimum Interoperability Software Suite

Fall 2020

Prepared by:
Ryan Baker, Engineering, IS90
December 3, 2020

Approved by:
End User Services Program Board
December 10, 2020

Revision History

Status	Version	Date	Author(s)	Summary of Change
Update	Spring 2020	03/27/2020	Troy Farsoun	Content updated. Standard migrated into new template.
Update	Fall 2020	12/3/2020	Troy Farsoun	Content updated.

Table of Contents

1. Scope **1**
1.1 Applicability 1
1.1.1 Assessments 1
1.2 Authority 2
2. General Requirements **2**
2.1 Architectural Compliance Requirements 2
3. Client Reference Configurations **3**
3.1 Default Operating Systems for NASA End Users 4
3.1.1 Windows Client Reference Configurations 5
3.1.2 Apple Client Reference Configurations 7
3.1.3 Red Hat (RHEL) Client Reference Configurations 8
3.2 Legacy and Sunsetting Operating Systems for NASA End Users 10
3.2.1 Windows Client Reference Configurations 10
3.2.2 Apple Client Reference Configurations 10
3.2.3 Red Hat (RHEL) Client Reference Configurations 10
3.3 Client Reference Configuration for Mobile Computing Systems 11
4. Operating Systems **11**
4.1 Operating System Standards, Timelines, and Compliance Dates 11
4.2 Microsoft Windows 11
4.2.1 Windows 10 11
4.3 Apple macOS 12
4.4 Linux 12
4.4.1 Red Hat 12
4.5 Mobile 12
4.5.1 Mobile Hotspots 14
5. Applications **14**
5.1 Office Automation Applications 14
5.1.1 Office Pro Plus for Windows 14
5.1.2 Libre Office 15
5.1.3 Collaboration Solutions 15
5.2 Electronic Messaging 15
5.3 Electronic Forms 15
5.4 SATERN 16
5.5 Virtualization 16
5.6 Optional Software for Mobile Computing Devices 16
6. Web Browsers **16**

6.1 Microsoft Internet Explorer 17
6.2 Microsoft Edge 17
6.3 Mozilla Firefox Extended Support Releases 17
6.4 Apple Safari 18
6.5 Google Chrome 18

7. ICAM Device Integration Configuration Requirements 18

7.1 Authentication Configuration Requirements 18

7.1.1 Linux PIV-M Solutions 18

7.2 NASA Client Trust Reference 19
7.3 NASA Trust Anchor Management 19
7.4 Content Encryption and Secure Email 19
7.5 Additional Relying Party Requirements 20
7.6 Additional Smartcard Middleware Requirements 20
7.7 Password Management 20

8. Security Requirements for NASA Systems 20

8.1 Agency Security Configuration Standards 21
8.2 Continuous Diagnostics and Mitigation 21

8.2.1 Configuration Settings Management and Software Asset Management ... 21
8.2.2 Allowlisting 21

8.3 Data Encryption 21
8.4 FIPS 140-2 Compliance Requirements 22

9. Network Requirements 22

9.1 Internet Protocol Version 6 Requirements 22
9.2 Network Access Control 23

9.2.1 Agency Virtual Private Network (VPN) Client 23
9.2.2 Network Access Control (NAC) Client 23

10. Compliance Requirements 24

10.1 Section 508 Compliance Requirements 24

10.1.1 Section 508 Tools 25

10.2 Energy Management Requirements 25

10.2.1 Computer Requirements 25
10.2.2 Printers 25

11. Basic Interoperability Standards Maintenance 25

12. Duration 25

13. Supporting Documents 26

14. Comments 26

Appendix A: Acronyms and Definitions 27

1. Scope

NASA-STD-2804, *Minimum Interoperability Software Suite*, defines the baseline software suite necessary to support interoperability and Federal technology compliance among NASA end user computing devices and within the NASA operating environment. This Standard establishes operating system configurations; application specifications; compliance dates for computers running Microsoft Windows, Apple macOS, mobile operating systems, and Linux operating systems; and other technical standard details within the NASA end user computing environment.

1.1 Applicability

This Standard is applicable to NASA End User Services Program Office (EUSO) Enterprise- and Center-managed systems at all NASA Centers, including Component Facilities and Technical and Service Support Centers. This Standard applies to the Jet Propulsion Laboratory (JPL)—a Federally Funded Research and Development Center (FFRDC)—and other non-Agency facility contractors only to the extent specified or referenced in applicable contracts. Center Chief Information Officers (CIOs) shall ensure that all NASA employees at their respective Centers have access to an interoperable system that is equipped with a minimum software suite that meets the guidance given in **Section 3** of this document.

NPR 2810.1x, *Security of Information Technology*, clearly defines the role and responsibilities of Information System Owners (ISOs) in maintaining Agency information systems. These responsibilities include:

- Acquiring, developing, integrating, operating, modifying, maintaining, and disposing of information systems.
- Ensuring system-level implementation of all Agency and Center requirements.
- Taking appropriate actions to identify and mitigate the risks associated with EUSO Information System Vulnerabilities and the impacts threats have on effected EUSO systems and the systems connected to EUSO systems

The Client Reference Configuration (CRC) in **Section 3** establishes required functionality and the required products necessary to meet minimum functionality. Licenses for products not included in the CRCs may not exist (particularly for Optional software) or may not be renewed. Products will be added, replaced, or removed as appropriate to address Agency interoperability requirements.

1.1.1 Assessments

Only core and optional software and hardware (as defined in this document) assessed by EUSO for end user interoperability prior to enterprise implementation shall be included in NASA-STD-2804 and NASA-STD-2805, *Minimum Hardware Configurations*. EUSO will provide overviews of current and planned activities, and will establish a registration process for end users and security stakeholders to participate in current assessments, as well as propose potential enterprise tools for future assessment.

Applications that meet common Agency end user technology needs while providing enhanced usability, mitigating security risks, reducing support costs, and/or offering other tangible and scalable improvements to the Agency may also be submitted for consideration in future revisions to these Standards.

When proposing assessments and additions, please keep in mind that the primary purposes of these Standards are to promote interoperability among all of NASA's computer systems and to provide common baselines of functionality and security that future Agency-wide applications can build upon. It is also important to note that this Standard applies to all interoperable end user systems throughout the Agency. Substantial costs may be involved in order to bring all Agency systems into compliance with an additional feature, particularly if the addition involves hardware. Cost vs. benefits must be carefully considered.

Each participant in EUSO assessment testing must be an Agency computing technology professional and must provide his or her own testing machine.

1.2 Authority

The Agency CIO has authorized EUSO to create binding technical standards related to Agency interoperability.

The NASA Technical Standards Program (NTSP), sponsored by the Office of the NASA Chief Engineer, recognizes EUSO as a standards-developing organization within the Agency. NTSP provides access to all technical standards at: https://standards.nasa.gov/

"Shall" statements in this document impose an obligation to act. "Shall not" statements generally prohibit an action. "Should" statements imply an obligation to act, but not a necessity.

Non-standard end user system configurations may be acceptable within the Agency environment if an Authorizing Official approves the deviation through a Risk-Based Decision (RBD) on the associated system security plan. RBDs are recorded in the Agency's system of record, Risk Information Security Compliance System (RISCS).

2. General Requirements

The following section outlines General Requirements.

2.1 Architectural Compliance Requirements

NPR 2800.1B, Section 4, Managing Information Technology, provides for a NASA Enterprise Architecture (EA) and Information Resource Management (IRM) Strategic Plan. Several facets of this Standard support the current NASA EA and IRM Strategic Plan:

- The selection of standards for a broad and cost-effective infrastructure using commercial off-the-shelf and well-supported open source products to the greatest extent practical
- Interoperability both within and when used remotely to NASA
- Flexibility for future growth
- Consistency with generally accepted consensus standards as much as feasible
- Security for NASA systems and data

In many cases, it is in NASA's best interest to specify commercial products as standard for an interoperable and secure implementation of a particular set of related and integrated functions. The products themselves often include additional functionality or proprietary extensions not specified by this Standard. While these products can be used to create higher-level interoperability solutions, these solutions may not be recognized as appropriate for interoperability or security within the context of the NASA interoperability environment and may be deprecated without warning by future revisions to this Standard. Users of this Standard are advised to apply appropriate caution when implementing proprietary or non-standard extensions and features that go beyond the explicitly stated functionality.

Per NPR 2800.1B Section 6, this standard also assumes consistent technology infrastructure exists at the individual Center level to support and maintain listed products and configurations.

3. Client Reference Configurations

To address application, data, and infrastructure interoperability, as well as ensure compliance with Federally-mandated system configuration settings, the software functionality, applications, interface standards, configuration settings, versions, and deployment settings established by this Standard are represented as Client Reference Configurations (CRCs).

The CRCs define the common enterprise images that system owners shall deploy to all interoperable end user computing systems. All IT initiatives funded or endorsed by the NASA OCIO presume systems that conform to the CRCs. Application service providers and software developers should use the CRCs to assist with integration and acceptance testing. Each CRC and corresponding applications are considered approved on the date of OCIO executive signing.

Operating systems and CRCs are now detailed between default and legacy / sunsetting statuses:

- Default configurations should be considered for all new and refreshed end user computing systems. These default configurations should meet the needs of most Agency end users and are intended to further modernize, standardize, and secure the Agency IT environment.
- Legacy/sunsetting configurations relate to operating systems that have been superseded by newer versions and/or are scheduled to lose functionality or

vendor support within the Agency environment. Mission or corporate considerations, such as a lack of critical mission or enterprise application interoperability with a default operating system, may necessitate some users retaining a legacy configuration, and/or seeking approval from an Authorizing Official to operate a non-standard system.

CRCs are included for each operating system, with the version numbers and required configurations that were current at the time of NASA-STD-2804 signing. Current available versions of listed applications must be used unless specifically stated otherwise. Interface standards are included to guide service providers and system integrators on specific application expectations. System administrators should deploy the latest version of a requested operating system unless the customer explicitly requests another supported version of the operating system.

Listed applications for each operating system are divided between Core and Optional CRCs:

- **Core**: A majority of users require these applications for a specific operating system. Prior to inclusion in 2804, EUSO assesses applications as part of holistic operating system builds and develops both standard configurations and security specifications that service offices and/or system owners must implement and support.
- **Optional**: These applications may appeal to a significant minority of NASA users for a specific operating system or provide notable performance differentiation over a Core application. These applications shall be made available by enterprise- or Center-based self-service tools when possible, but they may also be constrained by licenses or additional cost or support beyond that of a Core application. Support and security patching must be provided by offices and/or system owners, unless otherwise indicated.

NASA-STD-2804 is published twice each year, and current recommended versions of applications may change in between edits and signings of this Standard. Managers for corporate end user systems and enterprise management tools should consult current application versions for supported operating systems and ensure ongoing maintenance.

All operating systems and noted applications must adhere to Agency Security Configuration Standards (CSET) configurations and be removed from systems by listed end of life dates.

The Enterprise Service Desk (ESD) knowledge article “Base Services and General Services for NASA Enterprise Managed and Center Managed Systems” (KB0011257) clarifies applications and software in scope for non-enterprise licenses and support.

3.1 Default Operating Systems for NASA End Users

Windows 10 1909, macOS 10.15, and Red Hat Enterprise Linux 8 (RHEL 8) are the default operating systems for Agency end users.

3.1.1 Windows Client Reference Configurations

With Windows 10, Microsoft moved to a software-as-a-service model, providing release updates in a model called Semi-Annual Channel, formerly known as Current Branch for Business. Per Microsoft, this approach allows the vendor to provide smaller, more frequent feature updates with the intention of easing deployments and reducing enterprise implementation obstacles.

Channel releases are planned for twice each year, around March and September, with a lifecycle of roughly 18 months each. As new channels are released, Microsoft encourages enterprises to adopt them as soon as possible to achieve optimal security and interoperability. This Microsoft guidance currently drives EUSO assessments, channels selected for 2804 inclusion, and end-of-life-dates as they relate to Windows 10 channels.

Table 1. Windows 10 1909 NASA Core Build

Function	Application	Version	Comments & Required Removal Date
Operating System	Windows 10 Enterprise x64	1909 Semi-Annual Channel	
Applications, Plugins, and Tools			
Word Processing	Microsoft Word	Pro Plus ≥1902 / 2016	Use NASA-SPEC-2601APP.Office365 security specification.
Spreadsheet	Microsoft Excel	Pro Plus ≥1902 / 2016	Use NASA-SPEC-2601APP.Office365 security specification.
Presentation	Microsoft PowerPoint	Pro Plus ≥1902 / 2016	Use NASA-SPEC-2601APP.Office365 security specification.
Electronic Mail and Calendaring	Microsoft Outlook	Pro Plus ≥1902 / 2016	Use NASA-SPEC-2601APP.Office365 security specification.
Secure Electronic Mail	Entrust ESP Outlook Plug-in	10.x	
Instant Messaging	Microsoft Skype for Business / Microsoft Teams	Pro Plus / 2016	Skype support ends 07/2021
PDF Viewer and Electronic Forms	Adobe Acrobat Reader DC	2017	Default browser for opening PDF will be configured for Internet Explorer
Java	Java runtime environment (JRE)	≥ Java 8 update 241	Initiative to migrate to Java 11 began 03/2020
Web Conferencing	Microsoft Skype for Business / Microsoft Teams	Pro Plus / 2016 Teams 1.3.x	Skype support ends 07/2021
Backup Solution	Druva	6.6.x	
IPTV	Haivision Helper	1.2.x	
Browsers			
Web Browser	Microsoft Internet Explorer	11.x	Microsoft is dropping support for IE11 in Aug 2021 *for MS cloud services*, but the browser will still be available in the OS for compatibility reasons.
Web Browser	Microsoft Edge	≥ 84.x	
Web Browser	Google Chrome	≥ 86	
ICAM			
redContent Encryption	Entrust ESP for Windows	10.x	
Smartcard Middleware	ActivClient	7.1.x	DSI version 4.1.x
Trust Anchor Management	NASA Trust Anchor Management	2020.1	

Function	Application	Version	Comments & Required Removal Date
Security			
Firewall	Windows Firewall		
Anti-Virus and Anti-Malware	Symantec Endpoint Protection	14.x	
Data at Rest Full Disk Encryption	Microsoft BitLocker	SEE 11.x	For key escrow enablement: Center-managed device admins will need to install the SEEM client on respective device. Once installation is complete, the Windows 10 device will encrypt the drive with BitLocker, prompt the user for a PIN, and automatically send the recovery key to the SEEM server. If a BitLocker recovery key is required, the user only needs to contact the ESD Helpdesk.
Configuration Settings Management and Software Asset Management	IBM Endpoint Security (BigFix)	9.x	
Incident Monitoring and Response	FireEye HX	27.x	
IPTV	Haivision Helper	1.2.x	
Network Access Control	EIB NAC	Version is maintained by Communications Program and released via BigFix	

Table 2. Windows 10 1909 NASA Optional Supported Software

Function	Application	Version	Comments & Required Removal Date
Audio / Video Player	Microsoft Silverlight	5.1.x	Remove by October 12, 2021
Audio / Video Player	VLC	3.x	Authorized to support legacy video codec playback capabilities Compensates for Windows Media Player, which did not include legacy codecs like MPEG2 in this Windows 10 release.
Credential Vault Access	CA Privileged Access Manager (PAM) Client	2.8.2	PAM reference here differs from Pluggable Authentication Module discussed in **Section 7**.
File Archiver	7-Zip	19.x	
Text Editor w/ syntax highlighting	Notepad++	≥7.8	
PDF Creator	Adobe Acrobat Pro DC	2017	
Project Management	Microsoft Project	Pro Plus ≥1902 / 2016	
SFTP	WinSCP	5.x	Requires PuTTY-CAC and ActivClient for functionality
SSH	PuTTY-CAC	0.74	Requires WinSCP and ActivClient for functionality
Softphone Client and Instant Messaging	Cisco Jabber	12.x	
Virtualization	VMWare Workstation	15.x	

Function	Application	Version	Comments & Required Removal Date
Virtual Private Network	Cisco AnyConnect Security Mobility Client	4.9.x	Follows EBPro Guidelines defined by the Communications Program Office.
Web Browser	Mozilla Firefox Extended Support Release (ESR)	78.x	Versions after 52.x now only support browser extensions. NCFE is no longer supported and requires manual configuration. Instructions for Manual Smartcard Support
Web Collaboration	WebEx Productivity Tools	39.x	
Web Conferencing	WebEx Client	39.x	
Workflow	Microsoft Visio	Pro Plus ≥1902 / 2016	

3.1.2 Apple Client Reference Configurations

Table 3. macOS 10.15 NASA Core Build

Function	Application	Version	Comments & Required Removal Date
Operating System	macOS	10.15.x	
Mobile Device Management			
Mobile Device Management Client	Jamf Pro	Enterprise Managed: 10.24.x MOSM: 10.24.x	Jamf Pro configures and manages proper machine state, including configuration profiles and scripts associated with CSET specifications.
Applications, Plugins, and Tools			
Word Processing	Microsoft Word for Mac	Office 365 Business Pro 16.4x	Use NASA-SPEC-2601APP.Office365 security specification.
Spreadsheet	Microsoft Excel for Mac	Office 365 Business Pro 16.4x	Use NASA-SPEC-2601APP.Office365 security specification.
Presentation	Microsoft PowerPoint for Mac	Office 365 Business Pro 16.4x	Use NASA-SPEC-2601APP.Office365 security specification.
Secure Electronic Mail and Calendaring	Microsoft Outlook for Mac	Office 365 Business Pro 16.4x	Use NASA-SPEC-2601APP.Office365 security specification.
Instant Messaging	Microsoft Skype for Business / Microsoft Teams	Office 365 Business Pro 16.4x / Teams 1.3.x	Use NASA-SPEC-2601APP.Office365 security specification.
PDF Viewer and Electronic Forms	Adobe Acrobat Reader DC	2017	Default configuration to open will be Safari Browser
Java	Oracle Java Runtime Environment (JRE)	≥ Java 8 update 241	Java 11 migration is in progress
Multimedia Player	Apple iTunes	12.9.x	
Web Conferencing	Microsoft Skype for Business / Microsoft Teams	Office 365 Business Pro 16.4x / Teams 1.3.x	Use NASA-SPEC-2601APP.Office365 security specification.
Backup Solution	Druva	6.6.x	
IPTV	Haivision Helper	1.2.x	Use NASA-SPEC-2601APP.Haivision_Helper security specification.
Browsers			
Web Browser	Apple Safari	14.x	Use NASA-SPEC-2601APP.Safari security specification.
Web Browser	Google Chrome	86.x	Use NASA-SPEC-2601APP.Chrome security specification.
ICAM			
Authentication Client	Enterprise Connect PKI	2.x	Use NASA-SPEC-2601APP.Enterprise_Connect security specification.

Function	Application	Version	Comments & Required Removal Date
Trust Anchor Management	NASA Trust Anchor Management	2020.x Core and Optional	Installation Instructions: NASA Trust Anchor Management (NTAM) for Mac
		Security	
Firewall	Apple Firewall		
Anti-Virus and Anti-Malware	Symantec Endpoint Protection for Mac	14.3.x	
Data at Rest Full Disk Encryption	FileVault 2	FileVault 2	
Configuration Settings Management and Software Asset Management	IBM Endpoint Security (BigFix)	10.x	Use NASA-SPEC-2601APP.BigFix security specification.

Table 4. macOS 10.15 NASA Optional Supported Software

Function	Application	Version	Comments & Required Removal Date
Audio / Video Player	VLC	3.x	Use NASA-SPEC-2601APP.VLC security specification.
Content Encryption	Entrust Secure Desktop for Mac (SDM) 8.2	8.3.x	Use NASA-SPEC-2601APP.Entrust security specification.
Credential Vault Access	CA Privileged Access Manager (PAM) Client	2.8.2	PAM reference here is different from Pluggable Authentication Module discussed in **Section 7**.
Instant Messaging	Adium	1.5.10.x	Use NASA-SPEC-2601APP.Adium security specifications.
Project Management	ProjectLibre	1.9.x	Use NASA-SPEC-2601APP.ProjectLibre security specification.
Softphone Client and Instant Messaging	Cisco Jabber	12.x	Use NASA-SPEC-2601APP.Cisco_Jabber security specification.
Virtualization	VMware Fusion	12.x	VMWare Tools must be installed.
Virtual Private Network	Cisco AnyConnect Security Mobility Client	4.9.x	Use NASA-SPEC-2601APP.AnyConnect security specification.
Web Browser	Mozilla Firefox Extended Support Release (ESR)	78.4.x	Use NASA-SPEC-2601APP.Firefox security specification.
Web Collaboration	WebEx Productivity Tools	32.x	Provided for large and/or secure meeting use cases. See **Section 5.1.3** for Future Expected Updates. Use NASA-SPEC-2601APP.Webex security specification.
Web Conferencing	WebEx Client	40.0.6	Provided for large and/or secure meeting use cases. See **Section 5.1.3** for Future Expected Updates. Use NASA-SPEC-2601APP.Webex security specification.

3.1.3 Red Hat (RHEL) Client Reference Configurations

Like macOS and Windows, the Red Hat Enterprise Linux (RHEL) update schedule has major milestones. Due to the nature of the open source ecosystem, however, OS and software updates are not synchronized with the point releases. For this reason, it is important to maintain updates to RHEL systems on a continual basis and not just at point releases. Generally, point releases will bring new features, but security and stability updates come as they are completed by the community.

System owners shall use the most recent versions of software available that are compatible with a user's system configuration. If system owners are operating software that is not compatible with current OS versions or CSET Security Configuration Specifications, system owners will be required to submit an Agency Plan of Actions and Milestones (POA&M) that will identify coordination efforts with software vendors or application owners to updated software / applications to allow them to meet current NASA guidelines.

Table 5. RHEL 7.x NASA Core Build

Function	Application	Version	Comments & Required Removal Date
Operating System	Red Hat Linux Workstation	≥8.x Update source: Red Hat	In compliance with NASA kernel configurations.
Applications, Plugins, and Tools			
Office Automation	LibreOffice	≥5.3	
Secure Electronic Mail	Gnome Evolution	≥3.28	
Calendaring	Microsoft Outlook Web Access (NOMAD)		Accessible via web browser.
Instant Messaging	Pidgin	≥2.10	Requires pidgin-sipe plugin for Skype for Business.
Web Conferencing	MS Teams Web Access		
PDF Viewer	Evince Document Viewer	≥3.28	
Electronic Forms			No current standard solution. See **Section 5.3**
Java	Java Runtime Environment (JRE) – java-1.8.0-opendjk	≥ Java 8 update 241	
Backup Solution	Druva	6.6.x	
Browsers			
Web Browser	Google Chrome	80.x	
Web Browser	Mozilla Firefox Extended Support Release (ESR)	68.x	Versions after 52.x now only support browser extensions. Instructions for Manual Smartcard Support
ICAM			
Smartcard Middleware	Open SC	≥0.14	
Trust Anchor Management	NASA Trust Anchor Management	2020.1	Lacks auto-update Installation Instructions: NASA Trust Anchor Management (NTAM) for Linux
Security			
Firewall	firewalld	≥0.6.3	Used in conjunction with iptables.
Anti-Virus	ClamAV	Refer to the latest EPEL version.	
Data at Rest Encryption	Linux Unified Key Setup (LUKS)	≥2.0.3	No current escrow infrastructure.
Configuration Settings Management and Software Asset Management	IBM Endpoint Security (BigFix)	≥ 9.x	

Table 6. RHEL 7.x NASA Optional Supported Software

Function	Application	Version	Comments & Required Removal Date
Credential Vault Access	CA Privileged Access Manager (PAM) Client	2.8.2	PAM reference here is different from Pluggable Authentication Module, discussed in **Section 7**.
Virtual Private Network	Cisco AnyConnect Security Mobility Client	4.4.x	

3.2 Legacy and Sunsetting Operating Systems for NASA End Users

Operating systems are approaching end-of-life for Agency end users including Windows 10 versions below 1909 and Red Hat Enterprise Linux (RHEL) 7.6 (and below).

3.2.1 Windows Client Reference Configurations

Table 7. Windows Devices

Function	Application	Version	Comments & Required Removal Date
Operating System	Windows 10	1809, 1709, 1703, 1607, 1511	See https://cset.nasa.gov/ascs/software-life-cycle/#sunset-os for EOL dates.
Applications, Plugins, and Tools			
Word Processing	Microsoft Word Professional	2013	
Spreadsheet	Microsoft Excel Professional	2013	
Presentation	Microsoft PowerPoint Professional	2013	
Electronic Mail and Calendaring	Microsoft Outlook Professional	2013	

3.2.2 Apple Client Reference Configurations

Table 8. OS X / macOS Devices (macOS 10.15 NASA Core Build)

Function	Application	Version	Comments & Required Removal Date
Applications, Plugins, and Tools			
Word Processing	Microsoft Word for Mac	2013 / 2016	
Spreadsheet	Microsoft Excel for Mac	2013 / 2016	
Presentation	Microsoft PowerPoint for Mac	2013 / 2016	
Secure Electronic Mail and Calendaring	Microsoft Outlook for Mac	2013 / 2016	
Instant Messaging	Microsoft Skype for Business	2013 / 2016	

3.2.3 Red Hat (RHEL) Client Reference Configurations

Like macOS and Windows, the Red Hat Enterprise Linux (RHEL) update schedule has major milestones. Due to the nature of the open source ecosystem, however, OS and software updates are not synchronized with the point releases. For this reason, it is important to maintain updates to RHEL systems on a continual basis and not just at point releases. Generally, point releases will bring new features, but security and stability updates come as they are completed by the community.

System owners shall use the most recent versions of software available that are compatible with a user’s system configuration.

Table 9. RHEL Devices

Function	Application	Version	Comments & Required Removal Dates
Operating System	Red Hat Linux Workstation	≥8.0 Update source: Red Hat	

3.3 Client Reference Configuration for Mobile Computing Systems

Table 10. Client Reference Configuration for Mobile Computing Systems

Functionality	Application	Version	Required Settings
Operating System	iOS	14.1 or later	See https://cset.nasa.gov/ascs/software-life-cycle/#operating-systems
Operating System	Android	10.0 or later	Shall implement most recent monthly security patching available from Google (Android).
Mobile Device Management	MaaS360	iOS: 3.98 or later Android: 6.9 or later	

4. Operating Systems

The following section outlines Operating Systems.

4.1 Operating System Standards, Timelines, and Compliance Dates

CSET investigates and identifies the applications and operating system versions that are unsupported by the vendor. NASA SOC investigates threats in applications and operating systems that signify an imminent threat due to unpatched vulnerabilities. The software lifecycle status for supported software can be found on the CSET website.

4.2 Microsoft Windows

The Windows firewall must be enabled for all versions of the Windows operating system. All Windows systems must meet the NASA Baseline Security Configurations to ensure compliance with FISMA requirements.

4.2.1 Windows 10

The 64-bit version of Microsoft Windows 10 1909 Semi-Annual Channel is the only version of Windows approved for use. The 32-bit version of Microsoft Windows 10 may be installed to support non-64-bit-capable applications that only run on the 32-bit version. Long-Term Servicing Channel (LTSC) is not supported.

Table 11. Windows 10 End of Life Timelines

Version	End of Service
2004	12/14/2021
1909	05/11/2021
1903	12/08/2020
1809	5/11/2021
1803	5/11/2021

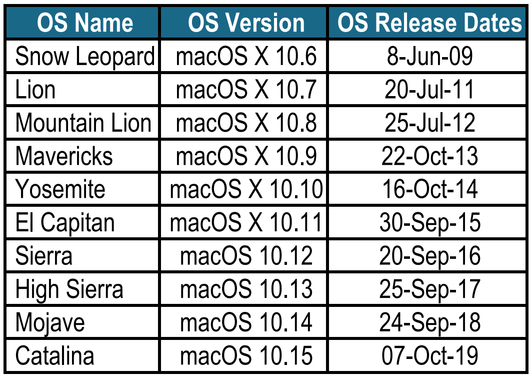
4.3 Apple macOS

Per the latest 2804 addendum, macOS 10.15 is approved for deployment on new and refreshed Mac hardware. It may optionally be deployed to existing Mac hardware.

Section 3.1.2 includes an application entry for Mobile Device Management (MDM) and the Jamf Pro client, which have been implemented by the Mac Operating System Management (MOSM) project. This client configures and manages proper Mac machine state and is a critical component of macOS 10.15 deployment and management. Refer to the EUSO / MOSM project schedule for updates on operational deployment.

For all versions of macOS operating systems, Apple FileVault must be enabled. All Apple systems must meet published NASA security configurations.

Table 12. macOS Timeline



OS Name	OS Version	OS Release Dates
Snow Leopard	macOS X 10.6	8-Jun-09
Lion	macOS X 10.7	20-Jul-11
Mountain Lion	macOS X 10.8	25-Jul-12
Mavericks	macOS X 10.9	22-Oct-13
Yosemite	macOS X 10.10	16-Oct-14
El Capitan	macOS X 10.11	30-Sep-15
Sierra	macOS 10.12	20-Sep-16
High Sierra	macOS 10.13	25-Sep-17
Mojave	macOS 10.14	24-Sep-18
Catalina	macOS 10.15	07-Oct-19

4.4 Linux

All new and refreshed Linux systems must run a supported RHEL distribution. Vendor-provided and -supported versions of applications shall be used. The version of application the vendor provides in their update stream shall supersede any listed in the CRC.

4.4.1 Red Hat

The default Red Hat Linux distribution for use on interoperable systems is Red Hat Enterprise Linux Desktop (RHEL) 8.0 with Workstation option on all new and refreshed systems. RHEL version releases prior to 7.6 are approved for use but will ***NOT*** be deployed to new or refreshed user systems. Any RHEL version lower than 7.6 must be removed from NASA user systems by November 30, 2020.

4.5 Mobile

The minimum iOS version is 14.1, and the current minimum Android version is 10.0.

Per ITS-HBK-2810.07-01, *Configuration Management*, Section 2, mobile systems by default are either moderate or high security posture, given that they may enter environments that pose significant risk. Mobile system owners shall ensure that devices within their scope incorporate an approved minimum operating system, or that deviations from approved minimum operating systems are recorded and approved in the corresponding system security plan, per the process noted in **Section 1.2**. Failure to deploy the minimum acceptable operating system or receive approval on deviations within a security plan may result in the removal of mobile systems' access to the Agency network.

Mobile operating systems shall apply NASA baseline security settings. All Android and iOS operating systems are required to be maintained to current supported vendor operating system versions.

With the implementation of the Mobile Device Management (MDM) project's Certificate Lifecycle Management (CLM) (Phase 2) for Enterprise-managed and Center-managed mobile devices, the following additional requirements shall apply:

- Enterprise-managed mobile users must enroll in MDM via Mobile Device Registration (MDR).
    - This requires the user have a PIV card. MDM delivers additional certificates to the device for email and Wi-Fi authentication and email encryption capability.
- MaaS360 secure container shall support NASA Microsoft Exchange email, calendar, and contacts.
- Centralized management via MaaS360 policies with specific support for remote wipe capability, certificate management, and secure container locking after predetermined number of bad passcode attempts must be enabled.
- A native network supplicant requirement for EAP-TLS authentication to support WiFi authentication shall be observed.
- NASA data shall not be stored or used outside of the MDM secure container.
    - NASA data are defined in the CIO's April 2018 "Use of Unauthorized Devices" memo as "information that is not publicly releasable and is in an electronic format that allows it to be retrieved or transmitted."
- Devices shall not be modified to circumvent the manufacturer's operating system security features (e.g., "jailbreak" or "root").
- A registered mobile device shall not be used as the sole repository for NASA data; this will assure NASA data are not irretrievable if the device is erased or lost.
- NASA-delivered apps, policies or configuration shall not be modified.
- Registered mobile devices which are lost, stolen, or compromised must be immediately reported to NASA's Security Operations Center at 1-877-NASA-SEC (1-877-627-2732).
- Any device registered as GFE within MDR is subject to application monitoring.
- CSET Security Specifications for the NASA MDM solution can be found at on the CSET website.

Future Expected Updates: The Mobile Application Management (MAM) project, Application Lifecycle Management (ALM), Phase 3, anticipates enabling mobile enterprise management of commercial off-the-shelf, government off-the-shelf, and custom enterprise applications utilized by NASA's workforce and stakeholders in phases during 2020–2021. Additionally, it is likely that only Apple (iOS) and Samsung (Android OS) mobile devices will be approved and supported in the Agency environment in the future. These manufacturers' native cryptography supports both Agency security standards and MDM requirements for third-party applications. Specific hardware details are included in NASA-STD-2805. Approved software and devices can be found at https://cset.nasa.gov/ascs/.

4.5.1 Mobile Hotspots

The EUSO Enterprise contract provides Wi-Fi hotspot options for Agency mobile users looking to enable network sharing with other NASA laptops and tablets. Please consult the EUSO Service Catalog.

5. Applications

The following section outlines Applications.

5.1 Office Automation Applications

The default document format for Microsoft Office and LibreOffice is the International Standards Organization's Standard Office Open XML format.

5.1.1 Office Pro Plus for Windows

Microsoft Office Professional Plus is approved for use and is the default office automation version on interoperable Windows systems. As part of the Office Pro Plus release, NASA is migrating to the 64-bit application package for Windows systems, but the 32-bit version of Office Pro Plus will be available due to vendors who only have 32-bit add-ins for Office Products.

Any user/organization that requires the installation of the 32-bit version in order to support internally run/managed applications will also be required to submit a Risk-Based Decision (RBD) and POA&M to address coordination with the vendor to update their application add-ins to support 64-bit.

Office Pro Plus is typically installed on Agency hardware by two methods:

- .exe install files (also known as Click-to-Run (C2R) files) are the default file type for Microsoft via the NASA O365 license agreement. Any users who is currently entitled and has a NASA O365 G3 license has by default Pro Plus available.

Office Professional Plus for Mac is approved for use and is the default office automation version on interoperable macOS systems. This application package is exclusively 64-bit.

5.1.2 Libre Office

Libre Office is approved for deployment on all interoperable RHEL 7.x systems. Data format interoperability and rendering issues between Microsoft Office and Libre Office continue to persist.

5.1.3 Collaboration Solutions

NASA currently has Office 365 Exchange, Skype OneDrive, and Office ProPlus available to enterprise-managed users, with additional services currently being implemented. These services will provide cloud-based, ITAR-capable storage and collaboration services, including team sites, unlimited storage, persistent team chat capabilities, and collaborative document editing for the NASA user base.

Future Expected Updates: The Box secure file sharing solution is completing its Agency pilot and is assessing next steps to achieve production implementation.

The Cisco WebEx service was moved to a FedRAMP tenant as part of the service transition to Communications Program / NASA Integrated Communications Services (NICS). NASA anticipates significant changes will be required to its software licensing approach and end user training and communications.

5.2 Electronic Messaging

The Agency NOMAD service provides integrated email, calendaring, scheduling, contact management, instant messaging, and web conferencing. All interoperable end user computing systems are required to be configured to access the NOMAD services.

The Identity, Credential, and Access Management (ICAM) should be able to support any email client that can leverage Microsoft ADAL authentication libraries or technologies for presenting interactive logon prompts which use https redirects. Any other authentication method will not work with the O365 email service.

5.3 Electronic Forms

The design and control of forms (Agency-level / NASA forms, Center forms, and organization forms) are addressed in NPD 1420.1, *NASA Forms Management*. NASA uses an Agency-wide, Adobe Experience Manager (AEM) solution that supports NASA business practices, embraces technology and innovation, and increases efficiency.

The NASA Electronic Forms System (NEFS) portal, which serves as the central repository for all Agency-level/NASA forms and Center-level forms, is available at https://nef.nasa.gov/.

To access and fill form templates designed via the AEM solution, end-user systems currently require the following applications on the Windows 10 or macOS 10.13/14/15 operating systems:

- Adobe Reader DC
- Standard NASA-supported browser (configured to open Adobe Reader DC PDF documents)
  - **Windows 10**: Microsoft Edge
  - **macOS 10.15**: Safari

Plug-ins or other external software are often incompatible with and/or break features of NASA forms (e.g., signing), as does using or manipulating them within applications like Mac Preview or third-party PDF editors. NASA forms are records and are intended to be used as-is with standard supporting software.

4-cert FIPS 201-2 smartcards are compatible with digital signature.

Linux operating systems and the Google Chrome and Mozilla Firefox browsers currently do not natively support Adobe Reader DC functionality.

5.4 SATERN

SATERN has been re-platformed to a Software-as-a-Service (SaaS) solution. NSSC has confirmed that this cloud-based, FedRAMP-approved solution will work with the standard operating systems and browsers included in **Section 3** of this document, which should provide additional access to Linux users, in particular.

5.5 Virtualization

Virtualization technology allows multiple operating systems to be run on a single physical computer. If a virtualization product is needed for interoperability, the current version of VMware for the respective operating system shall be used. The software listed in **Section 3**, **Client Reference Configurations**, for the virtualized operating system must be installed and configured as required by the system security plan.

5.6 Optional Software for Mobile Computing Devices

Optional software for mobile devices that provide useful functionality is available at: https://apps.nasa.gov/catalog

6. Web Browsers

No single browser meets the needs of the Agency. Google Chrome must be made available on all new or refreshed Windows, macOS, and RHEL interoperable end user systems. Internet Explorer and Edge Chromium (for Windows 10 only) shall be made available on Agency interoperable Windows systems; Safari shall be made available on Agency interoperable Macs; and Firefox ESR shall be made available on Linux systems.

To avoid inefficiencies and interoperability issues, NASA must adjust to the rapid pace of browser enhancements and new versions from the browser vendors. For Internet Explorer and Edge Chromium, NASA shall maintain support for the most recent production version. Chrome shall automatically update in the background as designed by Google. When employed as an optional browser, Firefox ESR shall be configured to automatically update with point releases for security updates.

Browsers should be configured with the Agency approved NASA Client Trust Reference (NCTR) list of trusted sites anchors. For additional information, see **Section 7**. Please refer to the internal IDI pages for all related up-to-date browser configuration guidance.

Web authors, application providers, and system integrators must ensure that their websites are validated against W3C Markup Validation Service and discontinue the use of checking client browsers for specific versions before granting access.

NASA Security Configuration Specifications shall be used for all approved browsers.

Web application developers should note that browser vendors have dropped support (or are dropping support) for Adobe Flash and Netscape Plugin Application Programming Interface (NPAPI), impacting plugins for Silverlight, Java applets, Facebook Live, and other similar applications. Chrome no longer supports NPAPI, and Mozilla has fully removed support for most NPAPI plugins in Firefox ESR.

6.1 Microsoft Internet Explorer

Internet Explorer is approved for use on interoperable Windows systems.

6.2 Microsoft Edge

Microsoft has re-written Edge based on the Chromium open-source project from Google. The new Edge browser replaces the original Edge that comes with Windows 10. CSET has written a security configuration specification for the new Edge browser, which can be found at https://cset.nasa.gov/specification/microsoft-edge-nasa-spec-2601app-edge-version-1-1/.

6.3 Mozilla Firefox Extended Support Releases

Mozilla Firefox ESR's NPAPI support was removed in fall of 2018, reducing its value differentiation within the Agency browser set. It continues to be the most difficult browser to integrate with ICAM services and smartcard-based authentication requirements.

Firefox configuration likewise has moved to Web Extensions exclusively and will no longer load other extension types. NASA Firefox Configuration Extension (NFCE) no longer functions without manual configuration, and EUSO support for the browser moving forward is unclear.

As a result, Firefox has been moved to the Optional CRC for Microsoft and Mac operating systems.

6.4 Apple Safari

Safari is approved for use on all interoperable macOS systems.

6.5 Google Chrome

Google Chrome is approved for use on all interoperable Windows, macOS, and Linux systems, and is intended as the browser with the most up-to-date features. The version of Google Chrome shall be continuously maintained by Google's automatic update process.

7. ICAM Device Integration Configuration Requirements

ICAM infrastructure services provide security controls for a significant portion of the core NASA operating environment. The following requirements have been identified for proper interoperability with ICAM services.

7.1 Authentication Configuration Requirements

The ICAM Device Integration (IDI) team develops software and configuration requirements for authentication with NASA standard operating systems. These configurations support such functions as:

- Smartcard-based authentication with the NASA PIV badge and other federally compliant smartcards, including non-NASA PIV, CAC, and PIV-I credentials.
- NASA Launchpad Simplified Logon
- Single-Sign-On with other Active Directory integrated applications such as:
  - Exchange and SharePoint
  - Project Server

All NASA personal computing devices running a full Windows, Mac, or Linux operating system shall have a built-in PIV smartcard reader or the ability to integrate a smartcard reader. EUSO will share IDI configuration requirements, which include settings for the operating system, browser, and middleware.

7.1.1 Linux PIV-M Solutions

As part of the OCIO PIV-M program, CSET engineered two Linux solutions to enable authentication compliance primarily on RHEL systems:

- **Pluggable Authentication Module (PAM)**: This solution enables enhanced PIV compliance primarily for unbound RHEL 7 workstations on the corporate network.
- **Secure Shell (SSH)**: This solution provides PIV compliance for network access via SSH on Linux systems (workstations/servers/jump hosts) capable of reaching NED.

Additional context and implementation details for these solutions may be found on CSET's handbook page.

7.2 NASA Client Trust Reference

The NASA Client Trust Reference (NCTR) repository for Trusted Sites can be found on CSET's ICAM Device Integration (IDI) site.

Trusted Sites are listed and or referenced in the NCTR when they are approved for deployment on NASA end user systems as required to enable Agency-level business functions for groups of personnel appreciably larger than those at any single NASA Center.

7.3 NASA Trust Anchor Management

Operating systems, as well as some third-party applications — such as Mozilla Firefox, Evolution, Adobe products, and Java — contain trusted certificate stores. The certificate stores are already preloaded and updated periodically by the product vendors with trusted certificates that are required for standard business functionality.

In addition to these vendor-supplied certificates, some of these certificate stores require additional certificates for interoperability with Agency and Agency affiliate services. This collection of additional certificates is managed through the enterprise NASA Trust Anchor Management (NTAM) effort. Reference National Institute of Standards and Technology (NIST) SP 800-52 Revision 1 for client configuration requirements for management of trust anchors. More information on NTAM can be found on the CSET website at https://cset.nasa.gov/idi/trust-anchor-management/.

7.4 Content Encryption and Secure Email

The NASA Operational Certificate Authority (NOCA) service provides PKI certificates for user authentication, encryption, and signing. User PKI certificates are encoded onto the NASA PIV and Agency Smart Badge (ASB) smartcards. Content and secure email encryption makes use of the public user certificates made available via the enterprise directory services, with the corresponding decryption performed by leveraging the private-keys from the smartcards.

For users who need additional content encryption, NASA ICAM PKI maintains secure desktop solutions for macOS and Windows making use of Entrust clients. The Client Reference Configurations include the appropriate Entrust client version for use in encrypting desktop files and an Outlook plugin for sending signed and/or encrypted messages.

For the latest required Entrust build, email client S/MIME configuration, and other smartcard information, please refer to the NASA ICAM PKI website

For situations in which a standard Entrust solution cannot be used to exchange sensitive information, you may contact the NASA ICAM PKI Team for alternatives.

NASA smartcards issued since September 2017 have additional storage for a longer encryption key history. Systems using these smartcards will require the latest middleware and post-issuance update software for proper functionality.

7.5 Additional Relying Party Requirements

All client applications that perform PKI operations shall support the SHA-2 family of algorithms. Information on SHA-2, RSA, and encryption algorithm lifetimes can be found in NIST Special Publication 800-78 Revision 4.

7.6 Additional Smartcard Middleware Requirements

The Desktop Smartcard Integration (DSI) Smartcard Middleware package for Windows systems provides full functionality for smartcard use in the NASA environment. This includes the ability to update smartcard certificates without having to go to a Center’s badging facility, integration for smartcard use with the Firefox browser, and support for FIPS 201-2-compliant smartcards. Other supported browsers have this functionality built in.

The most current version of DSI shall be installed by service providers via client reference configuration guidance in **Section 3**.

7.7 Password Management

NIST SP 800-63, Section 5.1.1.2, covers policy on Agency system storage of password credentials: “Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks. Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function”. Consult NIST SP 800-63 for details.

8. Security Requirements for NASA Systems

The ongoing utility and security of the NASA IT environment is directly dependent on a continuous stream of software and hardware updates. All NASA IT service providers shall enforce processes and solutions that minimize the time required to install updates and new versions of software. NASA-STD-2804 lists specific minimum versions of software required for compliance. Unless specifically indicated, NASA IT service providers and system administrators shall install minor updates throughout systems’ lifecycles and prepare major, tested new versions of software (including operating systems and browsers) in the shortest time possible.

The CRCs specify software and security settings required for access to the Agency IT environment. NASA IT service providers and system owners shall follow this guidance.

8.1 Agency Security Configuration Standards

NASA OCIO establishes Agency Federal Information Security Modernization Act (FISMA) compliance goals and reporting requirements for NASA systems using NASA security configuration specifications, managed by the Agency Security Configuration Standards (CSET) service. OCIO policy requires that NASA ASCS system configurations be deployed to all systems.

The NASA CSET security configuration specifications are internally developed by NASA and developed from various other sources, including the National Institute of Standards and Technology (NIST) checklists, Center for Internet Security (CIS) benchmarks, Department of Defense (DoD) Security Technical Implementation Guides (STIGs), and vendor and third-party sources. NASA's security configuration specifications, as well as their associated compliance monitoring measurement content, are managed by CSET.

NASA security configuration specifications for each operating system and applicable software listed in this Standard can be obtained at CSET (Agency Security Specifications Standards).

Centers seeking informed local consultation should contact their CSET Point of Contact.

8.2 Continuous Diagnostics and Mitigation

The Continuous Diagnostics and Mitigation (CDM) program is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

For more information on the CDM program schedule, please visit the CDM website.

8.2.1 Configuration Settings Management and Software Asset Management

As a component of the Federal government's CDM program, NASA uses IBM's BigFix to meet configuration and asset management reporting requirements.

8.2.2 Allowlisting

Future expected update: As a component of the CDM Program, NASA plans to enable AppLocker/Jamf Pro on all workstations, once operational. These pieces of software provide the ability to block any executable from running that is not on an Agency allowlist of approved software.

8.3 Data Encryption

All Agency systems shall implement a Data-at-Rest (DAR) encryption solution. Please refer to the CRCs in **Section 3** for specific operating system solutions.

DAR encryption solutions shall meet the following criteria:

- Cryptographic modules and other solution components must be FIPS 140-2 validated.
- Encryption keys must be managed and secured pursuant to NIST SP 800-57 Part 1 Rev 4 and NIST SP 800-53 Rev 4.
- Encryption keys must be centrally managed and escrowed to provide the ability for the Security Operations Center, law enforcement, the NASA Inspector General, and incident responders to access and recover data when necessary.

Additional DAR requirements are addressed in the Agency Security Configuration Standards, written by CSET and found here: https://cset.nasa.gov/ascs/.

8.4 FIPS 140-2 Compliance Requirements

NASA shall adhere to the guidelines and recommendations of the National Institute of Standards and Technology (NIST) as required by FISMA, particularly as they apply to computer security and encryption technology for hardware and software. More specifically, NASA shall comply with Federal Information Processing Standards (FIPS) 140-2 and 140-3 as validated encryption modules become available.

NASA application developers and service providers are reminded that cryptographic-based security systems being used to protect sensitive information in computer systems must be FIPS 140-2 validated. A current list of validated products can be found at: Cryptographic Module Validation Program

9. Network Requirements

The following section outlines Network Requirements.

9.1 Internet Protocol Version 6 Requirements

Internet Protocol version 6 (IPv6) is a newer version of the Internet Protocol, designed as the successor to Internet Protocol version 4 (IPv4).

All vendor laptops and desktops procured and distributed to NASA civil servants and contractors shall have IPv6 operating capabilities, confirmed by a Supplier's Declaration of Conformity. Vendor products should support Dynamic Host Configuration Protocol version 6 (DHCPv6). IPv6 configuration settings should remain in the operating system manufacturer default settings where IPv6 is enabled, unless systems are required to be transitioned to a modified Agency IPv6-enabled configuration. Detailed information on Federal requirements for IPv6 can be found at: Federal IPv6 Requirements.

Interoperable Agency systems should operate in dual stack — providing both IPv4 and IPv6 network capability — until further notice.

All new OCIO IT projects will now be required to document plans for supporting IPv6. Agency Program Management Office (APMO) System Engineering (SE) templates will be updated with IPv6 questions to assist in ensuring that appropriate IPv6 planning occurs.

9.2 Network Access Control

The following section outlines Network Access Controls.

9.2.1 Agency Virtual Private Network (VPN) Client

The External Border Protection (EBPro) project deployed a set of solutions (now part of the Trusted Internet Connection (TIC) Border Security Infrastructure) designed to improve the security posture of NASA’s networks and network-attached resources. Cisco’s Adaptive Security Appliance (ASA) is a component of that infrastructure. ASA supports the Agency Virtual Private Network (VPN) solution and requires installation of the Cisco AnyConnect Secure Mobility Client for end users to connect to the NASA network from remote locations.

As part of the Communications Program (CP) TIC Border Security Services, the Agency provides the Cisco AnyConnect Secure Mobility Client as the standard VPN client.

9.2.2 Network Access Control (NAC) Client

The Enterprise Internal Border - Network Access Control (EIB-NAC) project developed a solution for Network Access Control (NAC) based on the IEEE 802.1X network standard. The project installed the network infrastructure for NAC in monitoring mode, and the Agency is pursuing the goal of transitioning its networks to enforcement or “closed” mode. All devices attaching to any NASA network will eventually require some approved authentication and authorization method to access the network, either under the current NASA-initiated effort or via the Department of Homeland Security’s (DHS) Continuous Diagnostics and Mitigation (CDM) program.

Enterprise-managed Windows, Mac, and Linux devices must be configured for NAC in order to access to the NASA internal network. The design requires that a NAC client is installed on all NASA BigFix-enabled systems. The client manages certificate issuance for the device and configures the network interfaces to use device certificates for network authentication. A BigFix fixlet manages the delivery of the client and certificate to the end device.

Instructions for managing the client and certificate on end user devices is explained in the *NAC Enrollment Gateway Handbook* for the Device Admin role, found on the ICAM site in the NAC folder.

Client updates: As ICAM provides OCSS-approved NAC Client revisions, the version for each platform will be required to be installed on all in-scope devices. This will be managed via the BigFix process. Jamf Pro will be replacing BigFix for this process in the future.

10. Compliance Requirements

The following section outlines Compliance Requirements.

10.1 Section 508 Compliance Requirements

Software products procured after June 21, 2001, must be in conformance with Section 508 of the Rehabilitation Act.

In January 2017, the United States Access Board published a final rule updating accessibility requirements for Information and Communication Technology (ICT) covered by Section 508 of the Rehabilitation Act and Section 255 of the Communications Act.

Requirements apply to hardware that transmits information or has a user interface. Examples include computers, information kiosks, and multifunction copy machines. These provisions address closed functionality, biometrics, privacy, operable parts, data connections, display screens, status indicators, color coding, audible signals, two-way voice communication, closed captioning, and audio description.

Software requirements apply to computerized code that directs the use and operation of ICT and instructs ICT to perform a given task or function, including applications and mobile apps, operating systems, and processes that transform or operate on information and data. These provisions cover the interoperability with assistive technology, applications, and authoring tools.

Among other changes, the final rule emphasizes:

- Restructuring provisions by functionality instead of product type due to the increasingly multifunctional capabilities of ICT
- Requiring that operating systems provide certain accessibility features
- Clarifying that software and operating systems must interoperate with assistive technology (such as screen magnification software and refreshable braille displays)

Existing ICT, including content, that meets the original 508 Standards does not have to be upgraded to meet the refreshed standards unless it is altered. This “safe harbor” clause (E202.2) applies to any component or portion of ICT that complies with the existing 508 Standards and is not altered. Any component or portion of existing, compliant ICT that is altered after the compliance date (January 18, 2018) must conform to the updated 508 Standards.

This content was adapted from the United States Access Board Web site. For more final rule details, please visit: Access Board Final Rule

Complete NASA information and guidance on addressing Section 508 requirements are available at https://www.nasa.gov/accessibility/section-508-home

When developing and testing software, users should consider the tools in **Section 10.1.1** below, or more recent versions of these tools, for evaluation. These tools have been suggested for use by Agency users.

10.1.1 Section 508 Tools

Table 13. Section 508 Tools

Function	Windows	Mac	Red Hat Linux
Screen Reading Software	≥JAWS 2018.x	VoiceOver (Safari, Firefox, Chrome)	ORCA (Gnome package)
Screen Magnification Software	≥ZoomText Magnifier / Reader 2018 ≥ZoomText Fusion 2018	ZoomText Mac 1.2	Gnome shell, Magnifier, or xzoom
Speech Recognition Software		Dragon for Mac v6 (EOL, researching replacement prior to Spring 2021)	
PDF Documents	Adobe Acrobat, Reader DC, or Adobe Acrobat Pro DC	Adobe Acrobat Reader DC, or Adobe Acrobat Pro DC	

10.2 Energy Management Requirements

In order to comply with Executive Order 13693, *Planning for Federal Sustainability in the Next Decade*, printers and end user computing systems must be configured to use energy-saving settings.

10.2.1 Computer Requirements

- Displays must be set to sleep after 15 minutes of idle time.
- Systems shall go to sleep or hibernate after 60 minutes of idle time.
  - Generally, the level of sleep should be as effective as possible at saving power, given the constraints of the environment. To reduce power consumption to a minimum, the S4 power savings mode (suspend to disk) should be used.

10.2.2 Printers

All clients must be configured for duplex printing by default.

11. Basic Interoperability Standards Maintenance

This Standard will be reviewed and updated on an as-required basis, not to exceed two updates in a 12-month interval.

12. Duration

This Standard will remain in effect until cancelled or modified by the NASA CIO.

13. Supporting Documents

Supporting documents and additional information related to this Standard may be found on the CSET website.

14. Comments

NASA-STD-2804 includes information from teams and projects across the Agency. If outdated information from your team or project is referenced in the Standard, please review and provide updated information to your Center's CIO.

Appendix A: Acronyms and Definitions

Table 14. Acronyms and Abbreviations

Acronym/Term	Definition
ASA	Adaptive Security Appliance
ASCS	Agency Security Configuration Standards
ASUS	Agency Security Update Service
CA	Certificate Authority
CAC	Common Access Card
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CIS	Center for Internet Security
CRC	Client Reference Configuration
CSET	Cybersecurity Standards and Engineering Team
CSO	Communications Service Office
DAR	Data at Rest (encryption)
DHCPv	Dynamic Host Configuration Protocol version
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
DSI	Desktop Smartcard Integration
EBPro	External Border Protection Project
EMET	Enhanced Mitigation Experience Toolkit
ESD	Enterprise Service Desk
ESR	Extended Support Release (Firefox)
ETADS	Enterprise Technology Assessments and Digital Standards
EUSO	End-User Services Office
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FPKI	Federal Public Key Infrastructure
GFE	Government Furnished Equipment
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICAM	Identity Credential and Access Management
IDI	ICAM Device Integration
IE	Internet Explorer
IPv	Internet Protocol version
ISO	International Standards Organization
ITAR	International Traffic in Arms Regulations
IMAP	Internet Message Access Protocol
LUKS	Linux Unified Key Setup
MAPI	Messaging Application Programming Interface
MIME	Multipurpose Internet Mail Extension
NCAD	NASA Consolidated Active Directory
NCTR	NASA Client Trust Reference
NEFS	NASA Electronic Forms System
NFCE	NASA Firefox Configuration Extension
NIST	National Institute of Standards and Technology
NOCA	NASA Operational Certificate Authority
NOMAD	NASA Operational Messaging and Directory Service

Acronym/Term	Definition
NPAPI	Netscape Plugin Application Programming Interface
NTAM	NASA Trust Anchor Management
OASIS	Organization for the Advancement of Structured Information Standards
OCIO	Office of the Chief Information Officer
OCS	Microsoft Office Communications Server
PAM	Privileged Access Manager (Section 3)
PAM	Pluggable Authentication Module (Section 7)
PDF	Portable Document Format
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification - Interoperable
PKI	Public Key Infrastructure
POA&M	Plan of Actions and Milestones
RFC	Request for Comments
SATERN	System for Administration, Training, and Educational Resources for NASA
SCAP	Security Content Automation Protocol
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMTP	Simple Mail Transport Protocol
SSH	Secure Shell Protocol
SSL	Secure Sockets Layer
S/MIME	Secure/Multipurpose Internet Mail Extensions
STIG	Security Technical Implementation Guide
TLS	Transport Layer Security
VPN	Virtual Private Network
W3C	World Wide Web Consortium
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

Table 15. Definitions

Term	Definition
Basic Interoperability	Interoperability is the ability to obtain consistent and deterministic results within a specific platform (operating system software, minimum hardware, required and optional software), as well as between platforms (Windows, macOS, Linux), based on the established standards. Basic interoperability is also required with the Agency continuous monitoring/reporting tools in order to comply with Federal requirements.
End User Computing System	The term “End User Computing System” is used generically to refer to traditional desktop systems, as well as laptop computers, mobile devices, engineering workstations, and similar platforms that are used to provide basic interoperability.
Support for Basic Interoperability	Systems supporting basic interoperability are defined as Agency systems used to exchange information electronically by end users that require any of the functionality listed in **Section 3, Client Reference Configurations**.